

Debug service kết nối internet qua Prisma

Để kiểm tra kết nối từ máy chủ của 1MG đi ra internet hoặc đối tác bất kì cần thực hiện kiểm tra các thông tin sau:

Máy chủ đã đi qua Prisma chưa?

Kiểm tra bằng cách lấy IP public internet của máy chủ

Chạy 1 trong các lệnh curl sau để lấy ip public internet của máy chủ (thi thoảng 1 số curl sẽ bị rate limit):

```
curl ifconfig.me  
curl ipinfo.io/ip  
curl api.ipify.org  
curl ident.me
```

Nếu IP trả về là 66.159.198.25 => Đi qua Prisma

Nếu IP trả về trong danh sách sau, là đi qua CloudNAT

```
35.194.223.165  
35.221.215.24
```

Máy chủ đi qua CloudNAT sẽ không ăn firewall của Prisma → yêu cầu PIC Cloud của dự án tạo route qua Prisma.

Nếu máy chủ đi qua Prisma, Prisma đã cấu hình firewall đúng chưa?

Thực hiện lệnh `tcptraceroute` để kiểm tra route đã được thông tới đâu

Ví dụ máy chủ cần truy cập đến <https://example.com>, tương ứng với lệnh sau

```
sudo tcptraceroute example.com 443
```

Kết quả ra sẽ là:

```
Selected device ens4, address 10.255.134.204, port 32885 for outgoing packets
Tracing the path to example.com (93.184.216.34) on TCP port 443 (https), 30 hops max
 1  * * *
 2  10.124.35.254  1.350 ms  0.626 ms  0.584 ms
 3  * * *
 4  * * *
 5  ae-65.core1.sec.edgecastcdn.net (152.195.92.129)  127.974 ms  126.531 ms  126.387 ms
 6  93.184.216.34  126.147 ms  125.348 ms  125.275 ms
 7  93.184.216.34 [open]  126.279 ms  125.377 ms  125.161 ms
```

Trong đó IP 10.124.35.254 là IP của Prisma

Nếu sau khi đến 10.124.35.254 mà toàn * * * thì rule prisma đang có vấn đề, cần kiểm tra lại rule đã mở đúng chưa? PIC Prisma @ Trần Tuấn Anh (Deactivated)

Trường hợp kết nối đến với domain nhưng không thực hiện handshake được

```
[root@oracle-oem ~]# openssl s_client -showcerts -connect slack.com:443
CONNECTED(00000003)
write:errno=104
---
no peer certificate available
```

Có khả năng mở sai giao thức kết nối như nhầm https thành http nhờ PIC Prisma tiến hành kiểm tra lại rule xem đã mở đúng chưa

Nếu máy chủ đi qua Prisma, rule đã đúng, kiểm tra đối tác đã whitelist IP của Prisma chưa?

Thông thường đối tác cần whitelist 3 IP sau

IP Prisma:

66.159.198.25

IP CloudNAT (dự phòng):

```
35.194.223.165
35.221.215.24
```

Nếu đối tác whitelist lỗi, kết quả `tcptraceroute` thường qua 10.124.35.254 và 1 số hop, nhưng sau đó bị * * * nhiều.

Ví dụ:

```
Selected device ens4, address 10.255.134.204, port 32885 for outgoing packets
Tracing the path to example.com (93.184.216.34) on TCP port 443 (https), 30 hops max
 1  * * *
 2  10.124.35.254  1.350 ms  0.626 ms  0.584 ms
 3  * * *
 4  * * *
 5  ae-65.core1.sec.edgecastcdn.net (152.195.92.129)  127.974 ms  126.531 ms  126.387 ms
 6  93.184.216.34  126.147 ms  125.348 ms  125.275 ms
 7  * * *
 8  * * *
 9  * * *
```

Lúc này cần báo lại đối tác mở whitelist 3 IP:

66.159.198.25

```
35.194.223.165
35.221.215.24
```